Assurance Cases for Medical Devices

Charles B. Weinstock

April 28, 2011

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
28 APR 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Assurance Cases for Medical Devices	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Recently the U.S. Food and Drug Administration (FDA) issued guidance to infusion pump manufacturers recommending the use of an assurance case to justify claims of safety. An assurance case is somewhat similar in form and content to a legal case. It specifies a claim regarding a property of interest, evidence that supports that claim, and a detailed argument explaining how the evidence supports the claim. Assurance cases have been used in Europe for more than 15 years to argue safety cases for military, avionics, railway, and nuclear systems. The FDA is the first U.S. organization to officially encourage their use in assessing safety critical systems. This presentation will include a brief introduction to assurance cases, why they are useful, how they are developed, and how they can be used to help assure the safety of medical devices.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**52**	

SATURN 2011

Seventh Annual SEI Architecture Technology User Network Conference

Architecting the Future

May 16-20, 2011 | San Mateo County, California

The SEI Architecture Technology User Network (SATURN) Conference brings together experts to exchange best architecture-centric practices in developing, acquiring, and maintaining software-reliant systems.

7 Things You Need to Know About the Next 7 Years in Architecture.


Architecture is Not Just for Architects


Architecture, Agile Development, and Business Agility


Soft Skills for Architects


Service-Oriented Architecture (SOA) and Cloud Computing


Architectural Knowledge Management


Architecting to Meet Tomorrow's Global Challenges


Model-Driven Architecting

www.sei.cmu.edu/saturn/2011

Software Engineering Institute | Carnegie Mellon

in collaboration with IEEE Software

SEI Webinar Series

Keeping you informed of the latest solutions.

Software Engineering Institute | Carnegie Mellon

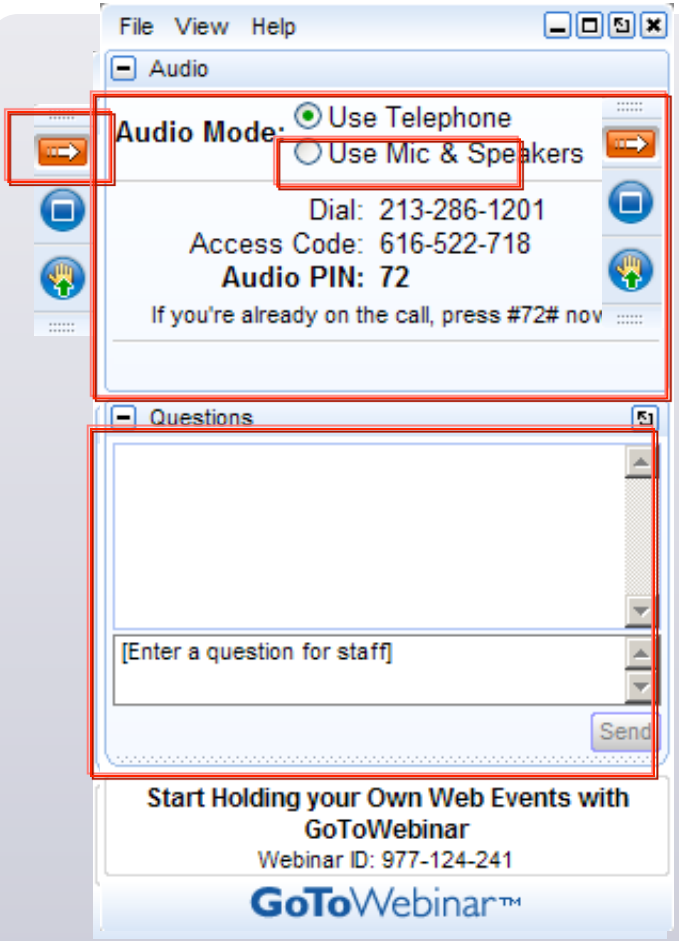
Join the SEI Webinar Series on LinkedIn

This forum allows attendees to discuss or post questions from the presentations in the SEI Webinar Series, and submit suggestions for future topics.

Search for Group:
SEI Webinar

www.linkedin.com

How to Participate Today



Open and close your Panel

View, Select, and Test your audio

Submit text questions

Q&A addressed at the end of today's session

Twitter: #seiwebinar

Today's Presenter

Chuck Weinstock has been with SEI for more than 25 years. He is currently a senior member of the technical staff in the System of Systems Software Assurance Initiative within the SEI's Research, Technology, and System Solutions program. With his colleague John Goodenough, Weinstock authored the 2009 SEI technical note *Towards an Assurance Case Practice for Medical Devices*. He has been active in the dependable computing field since the late 1970's when he worked at SRI International on the SIFT fault-tolerant computer. He earned a bachelor's degree in mathematics, a master of science degree in industrial engineering, and a doctorate in computer science, all from Carnegie Mellon University.

Software in Medical Devices

An ever increasing percentage of medical device functionality is provided by software.

- The industry is experiencing the problems which arise when hardware-intensive systems become software-intensive systems.

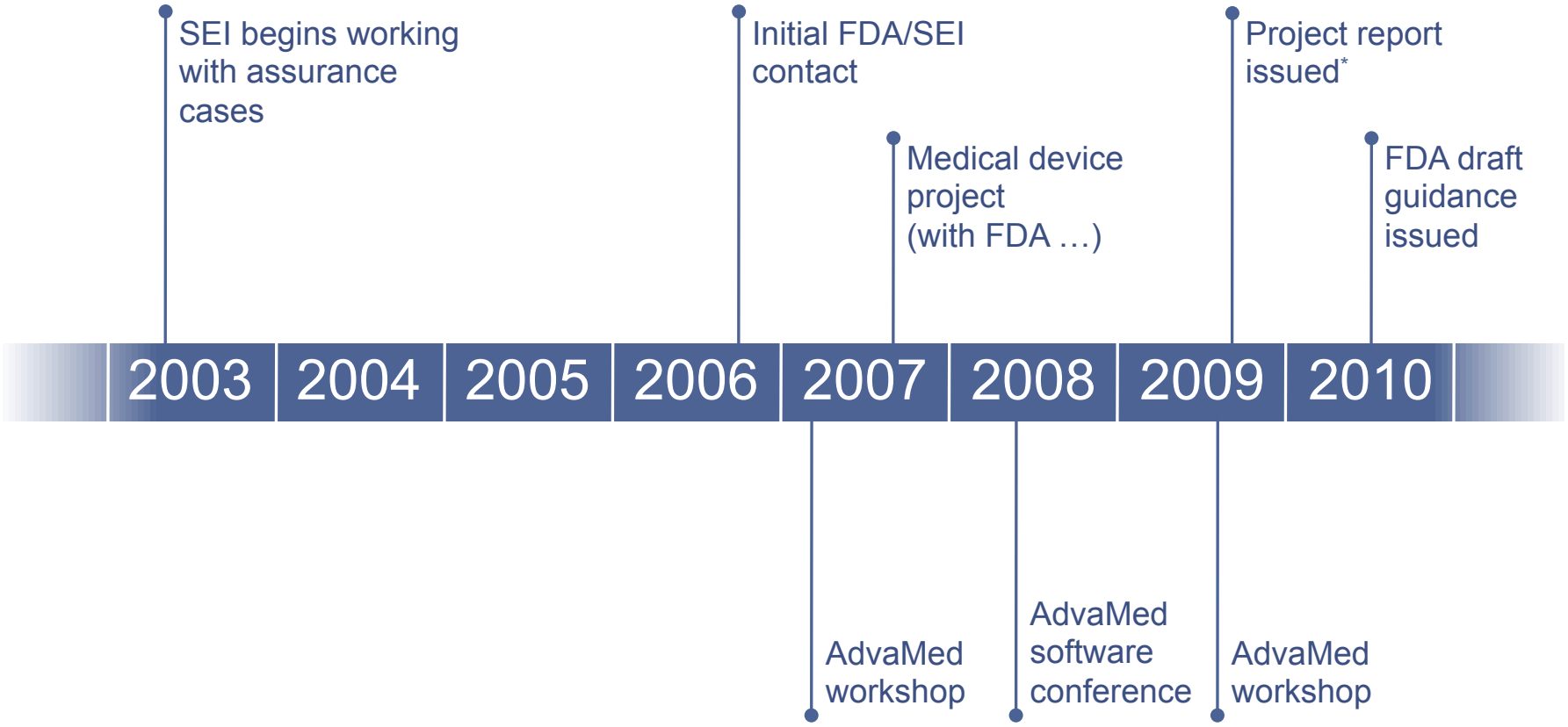
Specific concerns for medical devices include:

- Patient privacy (including HIPAA regulations)
- Safety
- Regulatory

A desire for more frequent “plug-and-play” (networked) use of the devices makes the problems particularly interesting.

- The patient is sometimes the network

The SEI and Medical Devices



*Charles B. Weinstock and John B. Goodenough, Towards an Assurance Case Practice for Medical Devices, CMU/SEI-2009-TN-018, http://www.sei.cmu.edu/reports/09tn018.pdf

Overview of the Talk


The assurance "problem”


The assurance case


Recent FDA guidance regarding assurance


Goal structuring notation with an example


Assurance case patterns and archetypes


Tooling for assurance cases


Concluding thoughts

Overview of the Talk

The assurance "problem”

The assurance case

Recent FDA guidance regarding assurance

Goal structuring notation with an example

Assurance case patterns and archetypes

Tooling for assurance cases

Concluding thoughts

Polling Question 1

Why are you attending this webinar?

1. My company has an immediate need to use assurance cases for a medical device
2. My company has an immediate need to use assurance cases, but not necessarily for a medical device
3. I've heard about assurance cases and want to find out more about them
4. Other

Assurance

Justified confidence that a system will function as intended in its environment of use

Why should we have confidence?

What evidence is there to support this confidence?

Why do we believe the evidence?

It is not enough to provide evidence without an explanation of its significance

Assurance

Justified confidence that a system will function as intended in its environment of use

"as intended" by the system's users as they are actually using it

- Different usage patterns are possible by different sets of users

This includes evaluating mitigations of possible causes of critical failures

- Minimize impact of unusual (or unexpected) operational conditions
- Minimize impact of vulnerabilities that can be exploited by hostile entities, especially in networked environments

Assurance

Justified confidence that a system will function as intended in its environment of use

The actual environment of use

The System Assurance Problem

Systems are getting more complex and more dependent on software

- Reaching sound conclusions about safety, reliability, etc. is getting harder

Traditional methods for evaluating dependable behavior (e.g., safety) are increasingly inadequate

- Too costly (in time and money) to test complex systems well
- Testing is not the best way of showing impact of subtle, but critical errors
- Test results, by themselves, do not show that a system has been well engineered to run adequately under untested conditions
  - ✓ FDA: "A convincing argument must be made as to why [the] engineering approach is sufficient"

We need better means of justifying confidence that a system will behave as intended

Recognition of the Assurance Problem

National Defense Industrial Association (NDIA) Top Software Issues (August 2006)

- Testing, by itself, doesn't assure the system (NDIA 5)
- Component level assurance (if possible) does not imply system level assurance. Exhaustive testing is not feasible. (NDIA 6)

National Research Council (NRC) Report: Software for Dependable Systems: Sufficient Evidence? (2007)

- Assurance that a system is dependable requires the construction and evaluation of a "dependability case" (claims, argument, evidence, expertise)
- For testing to be a credible component of a [case for dependability], the relation between testing and properties claimed will need to be explicitly justified

http://www.ndia.org/Content/ContentGroups/Divisions1/Systems_Engineering/PDFs18/NDIA_Top_SW_Issues_2006_Report_v5_final.pdf

Approaches to Establish Confidence in Systems

Standards-Based

- Evaluate developer competence based on conformance to process standards
- Examples: DO 178B for avionics safety, Common Criteria for security

Product-Based

- An “assurance case” approach based upon:
  - ✓ Claims about product behavior supported by evidence based on product analysis
  - ✓ Evidence linked to claims by an argument
- Example: Safety case

Polling Question 2

Have you or your company experienced situations where assurance techniques such as testing have proven inadequate?

1. Yes
2. No

Overview of the Talk

The assurance "problem”

The assurance case

Recent FDA guidance regarding assurance

Goal structuring notation with an example

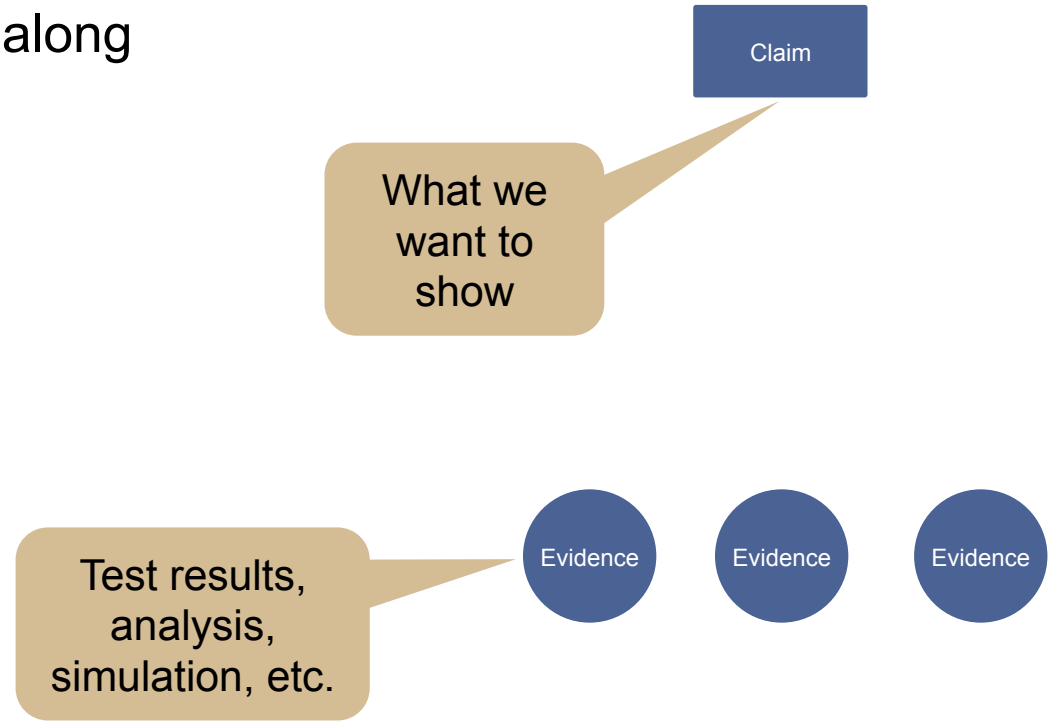
Assurance case patterns and archetypes

Tooling for assurance cases

Concluding thoughts

Assurance Cases

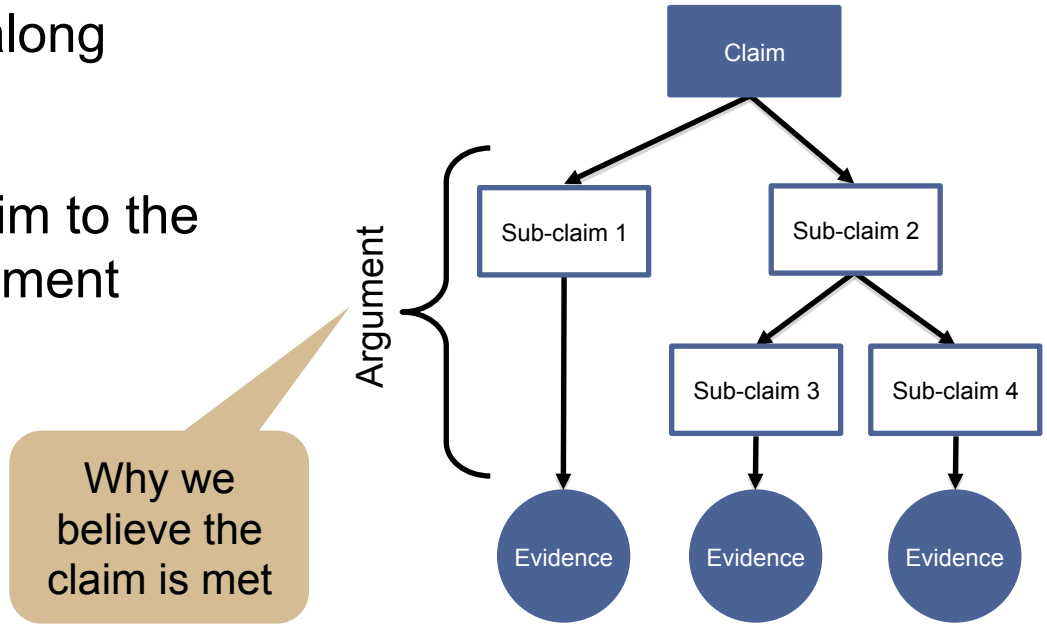
An assurance case presents a claim that a system is acceptably safe, secure, reliable, etc. in a given context along with supporting evidence



Assurance Cases

An assurance case presents a claim that a system is acceptably safe, secure, reliable, etc. in a given context along with supporting evidence

An assurance case links the claim to the evidence with a supporting argument



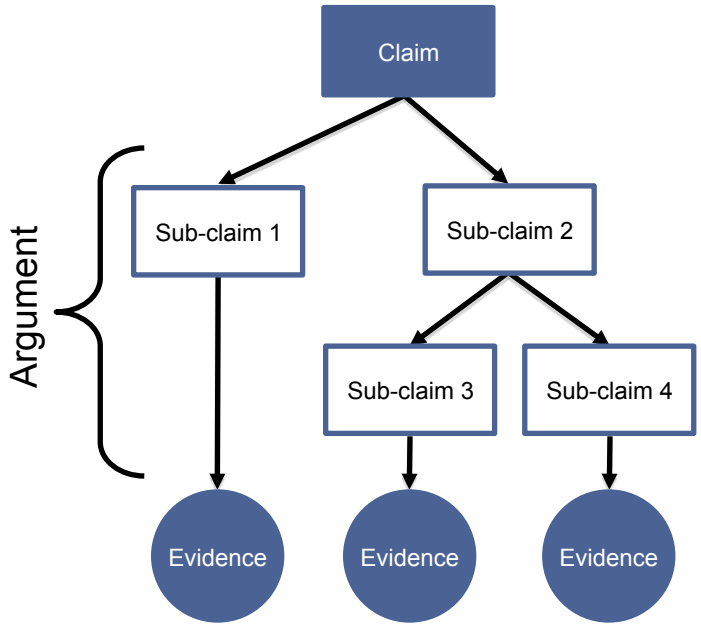
Assurance Cases

An assurance case presents a claim that a system is acceptably safe, secure, reliable, etc. in a given context along with supporting evidence

An assurance case links the claim to the evidence with a supporting argument

In general, the argument is broken down hierarchically

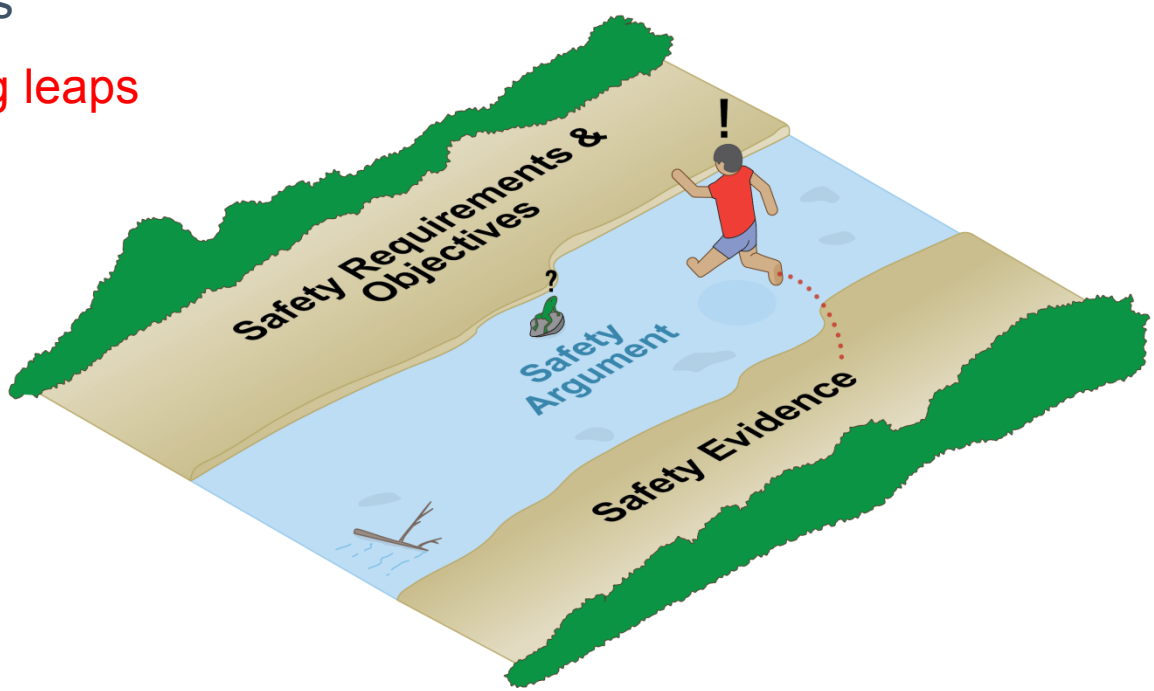
- Claims, argument, sub-claims, sub-arguments, evidence
- Easy to show graphically, although can be done in document structure (e.g., sub-section numbering)



The Argument Carefully Links Claims to Evidence

Important to “carry” the reader with you through the argument

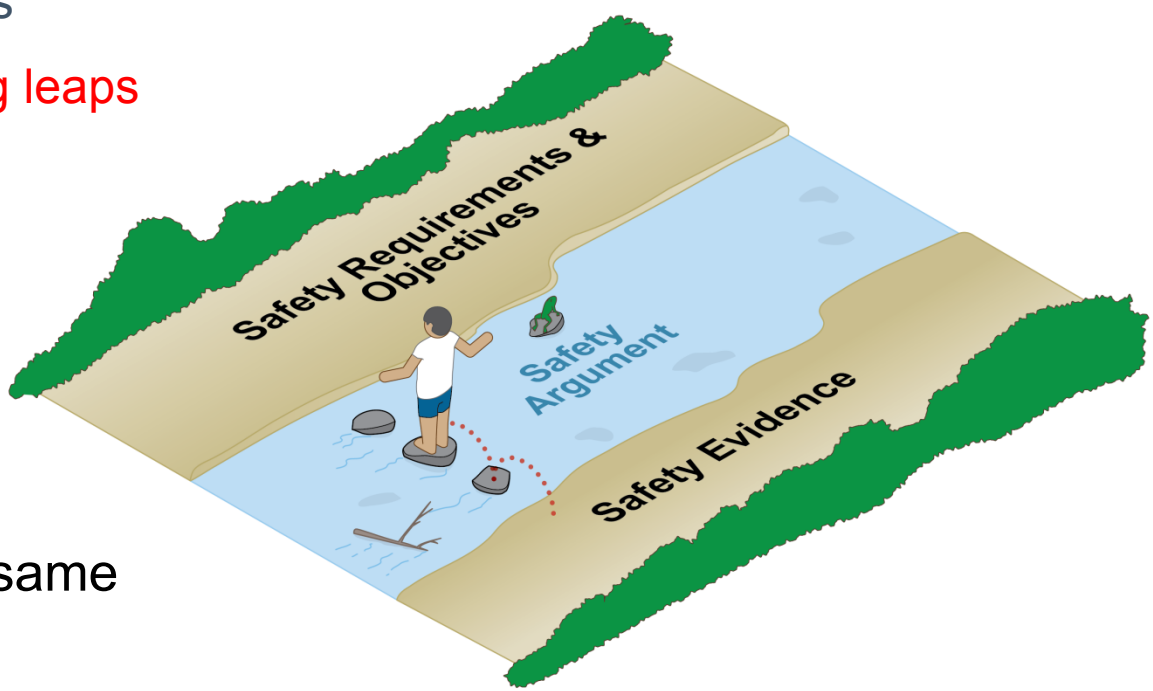
- Not lose them in the details
- Not force them to make big leaps



The Argument Carefully Links Claims to Evidence

Important to “carry” the reader with you through the argument

- Not lose them in the details
- Not force them to make big leaps



Need sufficient, judiciously placed stepping stones

Not all arguments need the same number of stepping stones

The FDA is finding insufficient “stepping stones” in current submissions

Overview of the Talk

The assurance "problem”

The assurance case

Recent FDA guidance regarding assurance

Goal structuring notation with an example

Assurance case patterns and archetypes

Tooling for assurance cases

Concluding thoughts

What is an infusion pump?

An infusion pump injects continuously or periodically, drugs, nutrients, or other injectable fluids into the circulatory system.

All infusion pumps require caregiver programming of the rate of injection and the length of time to deliver the fluid.

More complex pumps take into account the specific drugs being infused, the weight/age of the patient, and the hospital setting.

Some pumps allow the patient to control part of the injection process (e.g. to inject more painkiller).

Correct functioning of the pump is critical to the proper care of the patient.

FDA Guidance on Infusion Pumps

FDA draft guidance issued in April 2010 was intended to improve the quality of infusion pumps and reduce the number of recalls and Medical Device Reports.

- Demonstration of substantial equivalence via the use of an assurance case
  - ✓ Hazard areas of particular concern include: operational, environmental, electrical, hardware, software, mechanical, biological, chemical, and use
  - ✓ Information security: confidentiality, integrity, availability, and accountability
  - ✓ Risks to health: underdose, air embolism, overdose, incorrect therapy, etc.
  - ✓ Design and development decisions that bear on safety and effectiveness

http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm206153.htm

What is a Safety Argument

- **This infusion pump is safe because**
  - **The safety requirements are defined in my**
    - **Safety requirements analysis, derived requirements ...**
    - **Legislation, policy …**
- **The safety requirements are met through our**
  - **Safety analysis of design, use …**
  - **Hazard management through problem reporting**
  - **Observing failures are at a 'safe' level**
  - **Appropriate quantity, quality and rigor of evidence**
- **Safety management continues to be adequate because we have**
  - **SMS**
  - **staff competence**
  - **ongoing independent scrutiny ...**

http://www.fda.gov/downloads/MedicalDevices/NewsEvents/WorkshopsConferences/UCM219685.pdf

Assurance Cases for Safety

A means of justifying confidence that a system will be safe

- Augments testing where testing by itself is inadequate or too costly
  - ✓ Cannot demonstrate system safety/security/performance solely by testing
  - ✓ The FDA no longer wants to rely primarily on a hazard analysis and just test results to show that hazards have been adequately mitigated

Used extensively in developing safety-critical systems (in Europe)

Increasing interest in US

- FDA Infusion Pump Guidance [draft]
- NRC Report: “Software for Dependable Systems: Sufficient Evidence?”
- ISO 15026-2 “Assurance Case” [under development]

Overview of the Talk

The assurance "problem”

The assurance case

Recent FDA guidance regarding assurance

Goal structuring notation with an example

Assurance case patterns and archetypes

Tooling for assurance cases

Concluding thoughts

Goal Structuring Notation (GSN)

Was developed to help organize and structure Safety Cases in a readily reviewable form

Has been successfully used for over a decade to document safety cases for aircraft avionics, rail signaling, air traffic control, and nuclear reactor shutdown

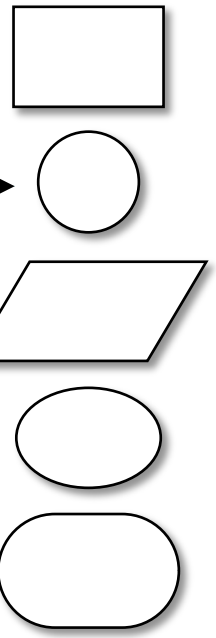
Shows how **claims** are broken down into sub-claims,

and eventually supported by **evidence**

while making clear the argumentation **strategies** adopted,

the rationale for the approach (**assumptions, justifications**)

and the **context** in which claims are stated



Example: Partial Requirements

5. Power and Battery Operations

5.1. Battery voltage

5.1.1. An active battery voltage shall be measured for the pump throughout its operation.

5.1.2. The active battery voltage shall be calculated as an average of 10 consecutive battery voltage readings.

5.1.3. The amount of battery life remaining shall be calculated as a function of the active battery voltage.

5.1.4. If the battery life remaining is less than *15 minutes*, the pump shall issue a Low battery alarm.

5.1.5. The low battery alarm shall be silenced when the pump is connected to an external power supply.

5.1.6. If the battery life remaining is less than *5 minutes*, the pump shall issue a Battery depleted alarm.

Example: Partial Hazard Analysis

1. Operational Hazards

HID	Hazard	Pump Type	Cause	Action	Mitigated by	Safety Requirement
1.1	Overinfusion	All	Programmed flow rate too high	Alarm(); Log()	Drug library	1.1, 1.4.4, 1.4.11
1.2	Overinfusion	All	Dose limit exceeded due to too many bolus requests	Alarm(); Log()	Flow sensor	1.4, 3.4.6
1.3	Overinfusion	All	(Programmed) Bolus volume/concentration too high	Alarm(); Log()	Drug library	1.4, 3.4.6
1.4	Overinfusion/ Underinfusion	All	Incorrect drug concentration specified	Alarm(); Log()	Barcode scanner	1.1, 6.1.3, 6.1.4

2. Environmental Hazards

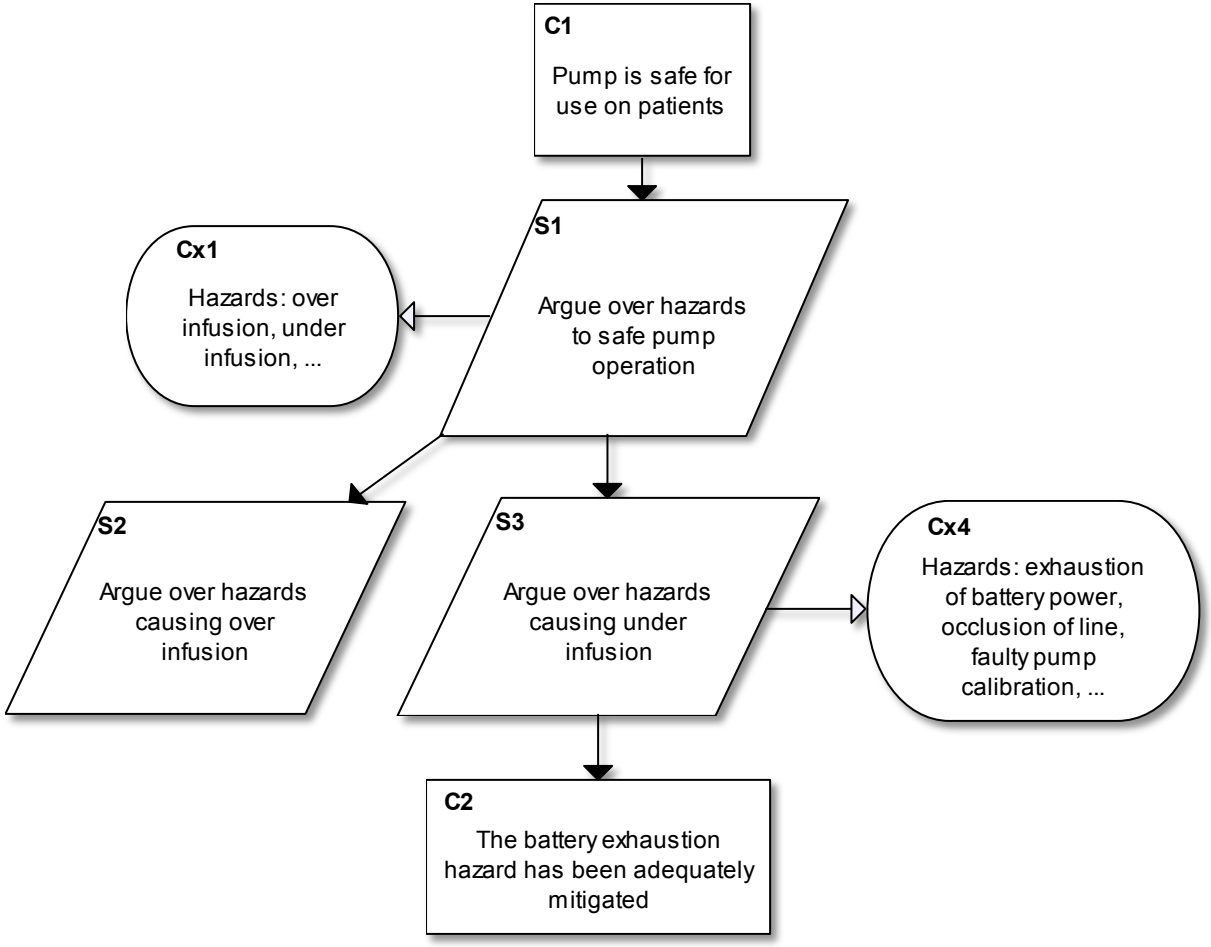
HID	Hazard	Pump Type	Cause	Action	Mitigated by	Safety Requirement
2.1	Failure to operate/ Pump malfunction	All	Temperature /Humidity/ Air pressure too high or too low			7.1
2.2	Contamination	FRN	Contamination due to spillage / exposure to toxins			

3. Electrical Hazards

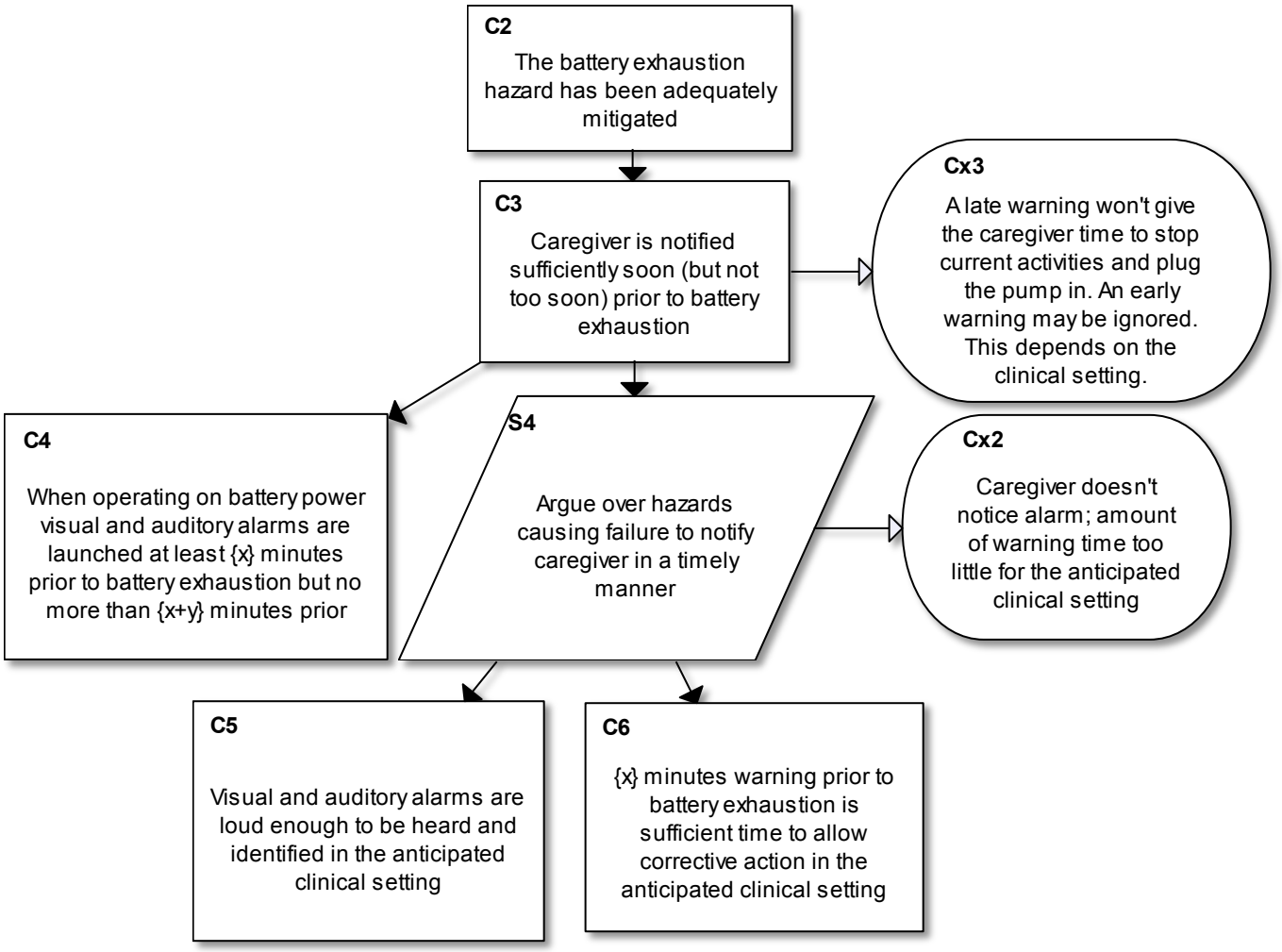
HID	Hazard	Pump Type	Cause	Action	Mitigated by	Safety Requirement
3.1	Overheating	FRN	Incorrect or loose interconnections between devices – channel error;	Alarm(); Log()		7.1.2
3.2	Overheating	FRN	Supply processor charge too high; Insufficient cooling/faulty heat sink; Unintended magnet quench	Alarm(); Log()		7.1.2, 7.3
3.3	Charge Error	All	Battery could not be charged	Alarm(); Log()		4.1.8
3.4	Supply Voltage Error	FRN	Supply voltage too high; Supply voltage too low; Battery voltage exceeds limits			7.3
3.5	Battery Failure	FRN	Battery voltage too low; Battery depleted	Alarm(); Log()		4.1, 5.1

Source: Hazard Analysis for the Generic Infusion Pump (University of Pennsylvania)

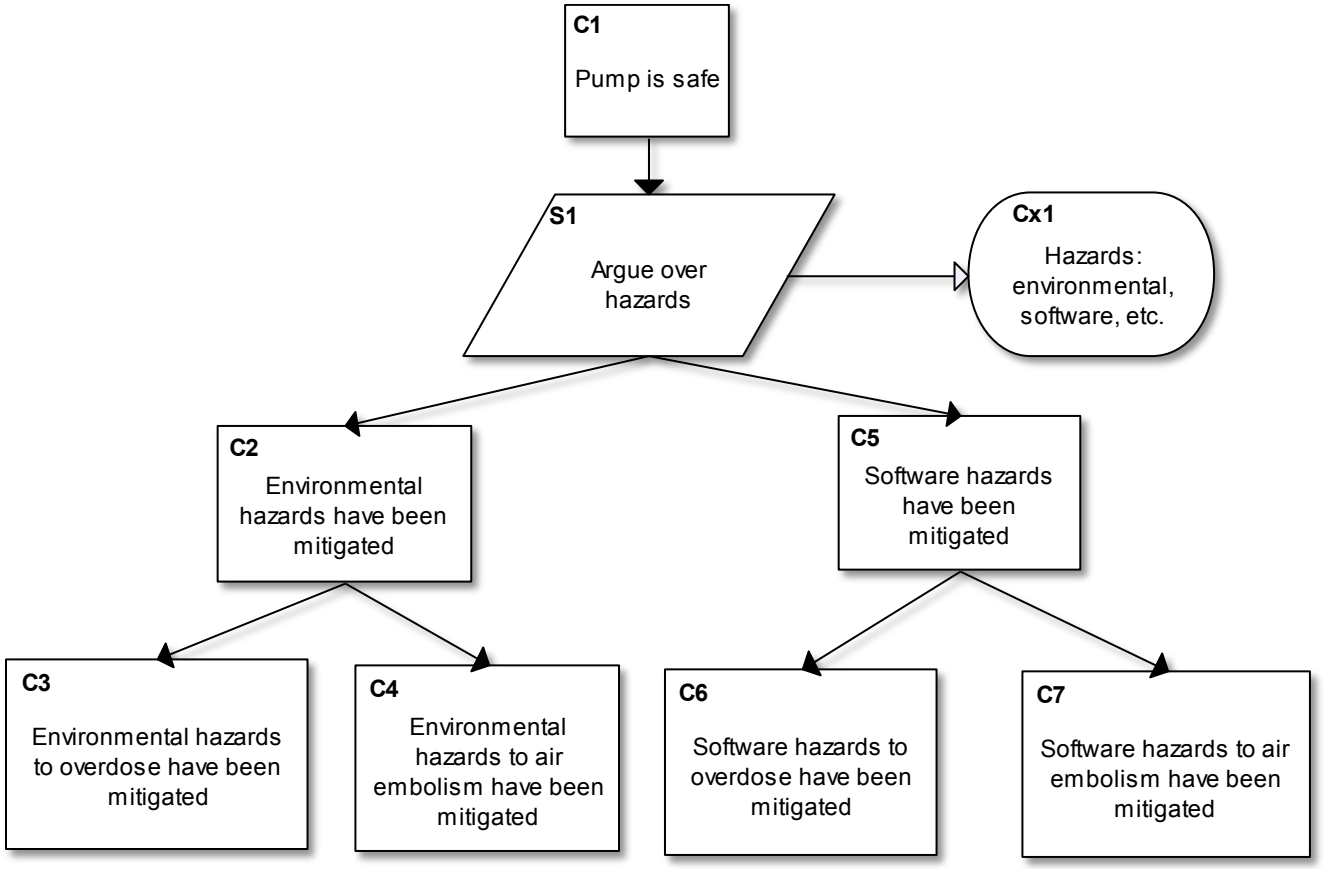
Example: Battery Exhaustion – Part One



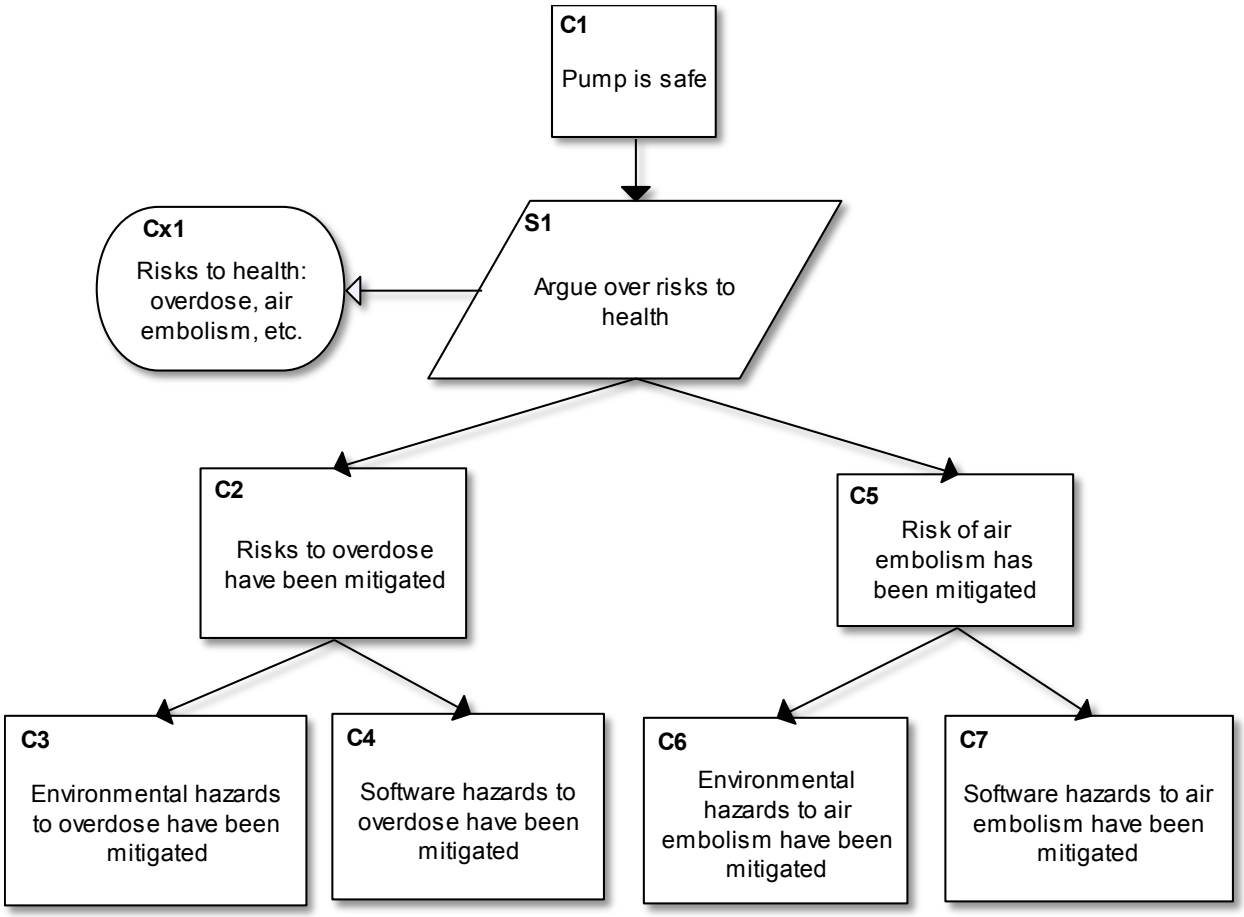
Example: Battery Exhaustion – Part Two



Two Ways to Structure: Arguing by Hazards to Safety



Two Ways to Structure: Arguing by Risks to Health



Assurance Case Benefits

Improves comprehension of existing arguments

Improves discussion and reduces time-to-agreement on what evidence is needed and what the evidence means

(Having identified argument structure up front) focuses activities towards the specific end-objectives

Recognition and exploitation of successful (convincing) arguments becomes possible (assurance case patterns)

Supports monitoring of project progress towards successful certification

When problems arise it helps with diagnosis

When new functionality is added it can quickly pinpoint needed new evidence (and identify existing evidence that need not be reconsidered)

Overview of the Talk

The assurance "problem”

The assurance case

Recent FDA guidance regarding assurance

Goal structuring notation with an example

Assurance case patterns and archetypes

Tooling for assurance cases

Concluding thoughts

Patterns and Archetypes

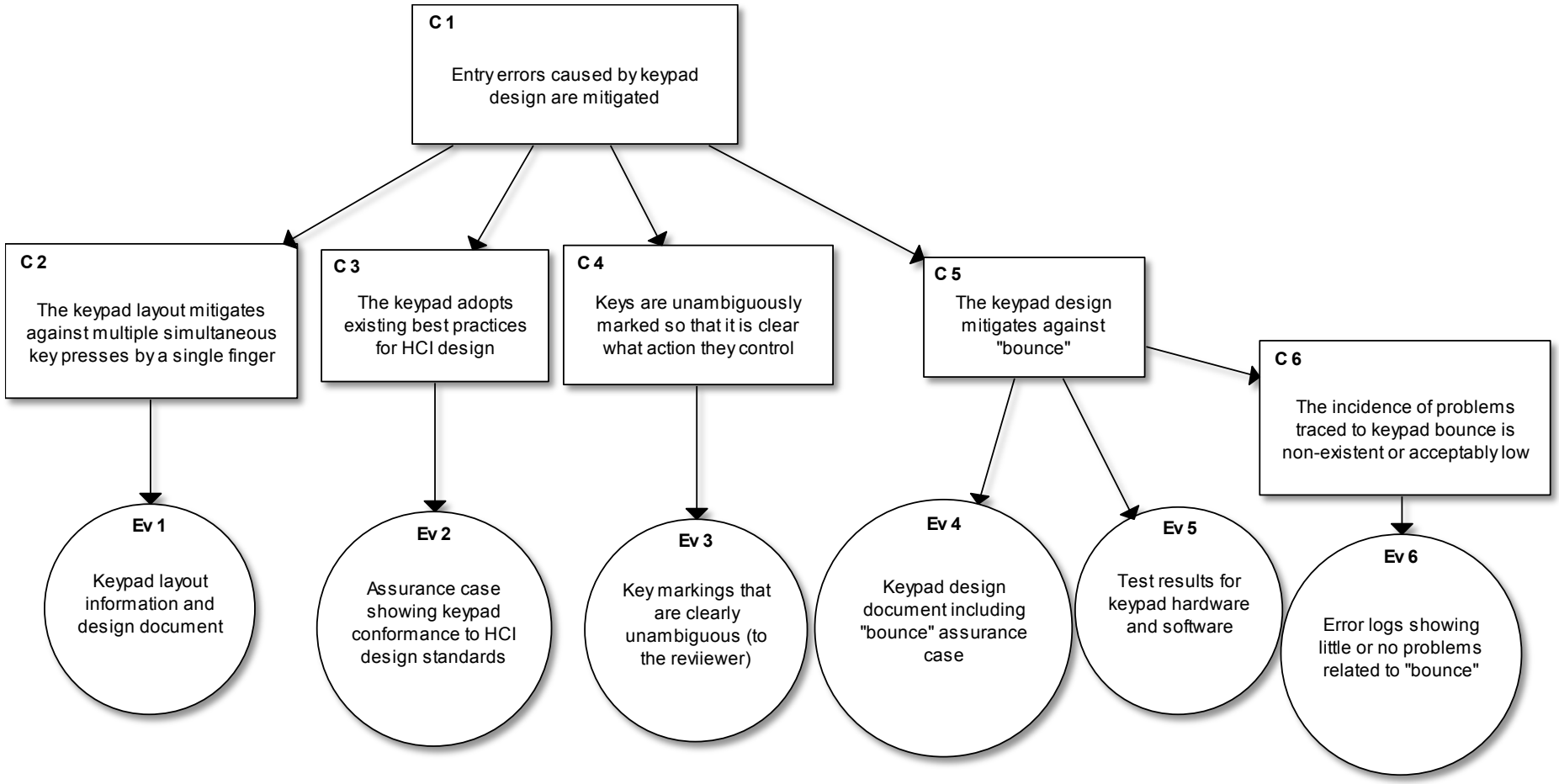
An assurance case pattern is a reusable template that captures acceptable ways of structuring a generic argument.

- Parameterized.
- Saves development time and money.
- For the FDA, saves valuable evaluation time.

A library of assurance case archetypes (patterns representing fragments of arguments) would have significant benefits:

- Guidance for the medical device manufacturer as to the proper argument and, perhaps more importantly, the required evidence.
- Ease the transition of the community to the widespread use of assurance cases.
- As long as the archetype argument applies the manufacturer and the FDA could treat the evidence as a check list.

Keyboard Archetype



Using the Archetype

A manufacturer developing a device with a keypad that conforms to the keypad archetype can:

- Assert that the keypad archetype argument applies
- Provide a checklist of evidence (with the evidence to back it up of course)
  - ✓ The keypad design has proper spacing
  - ✓ The keypad conforms to best HCI practice
  - ✓ The key markings are easily readable and unambiguous
  - ✓ The keypad design avoids “bounce”
  - ✓ A history that they keypad (or similar keypads) are trouble-free

The FDA can review the device without ever looking at the argument, but has it available if necessary.

Overview of the Talk

The assurance "problem”

The assurance case

Recent FDA guidance regarding assurance

Goal structuring notation with an example

Assurance case patterns and archetypes

Tooling for assurance cases

Concluding thoughts

Tooling

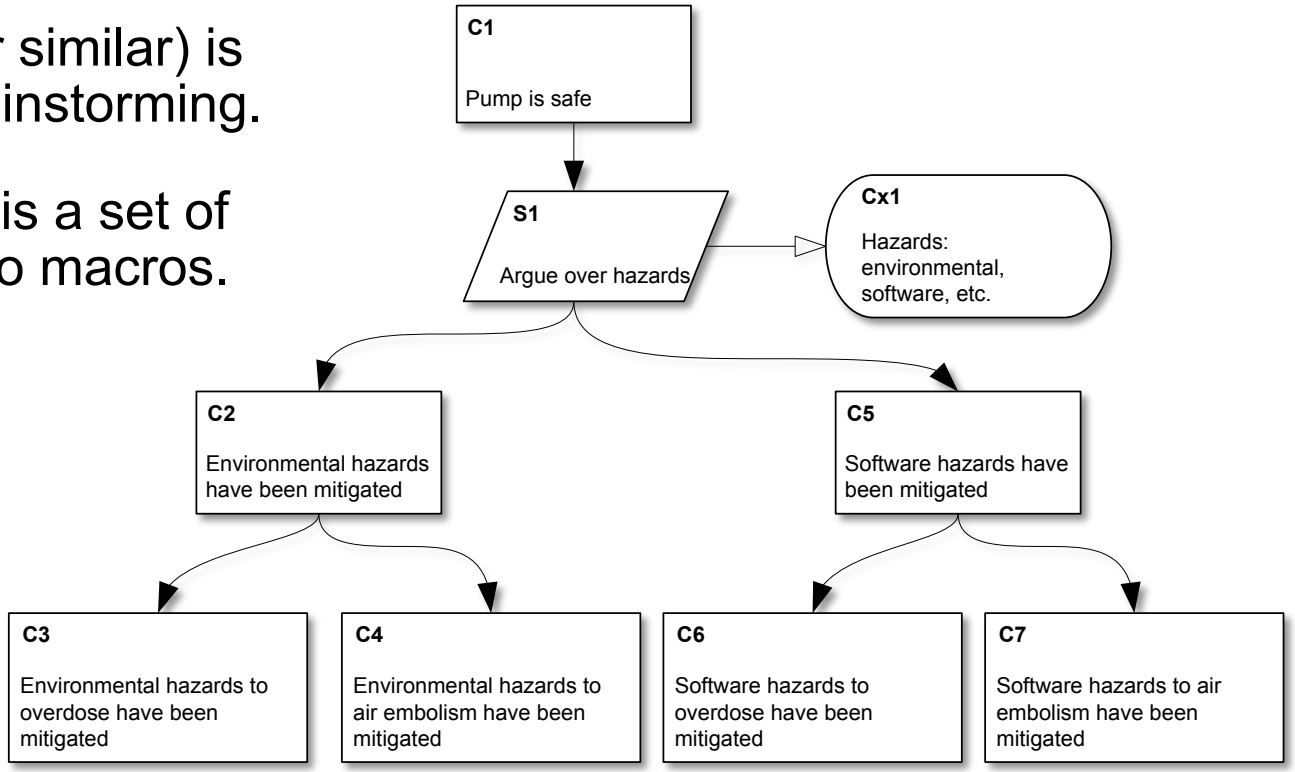
Goal structured assurance cases can be done with a word processor, but they are easier to follow when presented graphically. We've used three tools to produce assurance cases:

1. Mindmanager (or similar) is very good for brainstorming.

Tooling

Goal structured assurance cases can be done with a word processor, but they are easier to follow when presented graphically. We've used three tools to produce assurance cases:

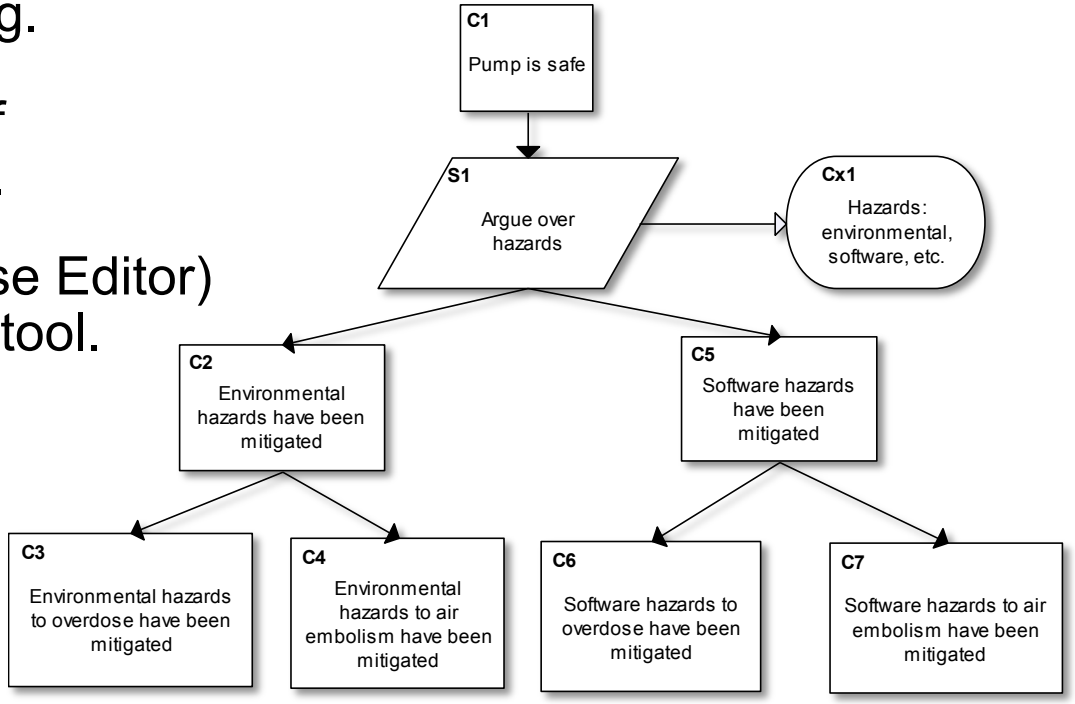
1. Mindmanager (or similar) is very good for brainstorming.
2. GSNCaseMaker is a set of unsupported Visio macros.



Tooling

Goal structured assurance cases can be done with a word processor, but they are easier to follow when presented graphically. We've used three tools to produce assurance cases:

1. Mindmanager (or similar) is very good for brainstorming.
2. GSNCaseMaker is a set of unsupported Visio macros.
3. ASCE (Adelard Safety Case Editor) is a supported standalone tool.



Overview of the Talk

The assurance "problem”

The assurance case

Recent FDA guidance regarding assurance

Goal structuring notation with an example

Assurance case patterns and archetypes

Tooling for assurance cases

Concluding thoughts

Implications for manufacturers

- The Safety Case will evolve over the life of the system
- While the structure of the Safety Case will broadly remain constant,
  - the status of the evidence will change, e.g., planned test coverage will be replaced by evidence of test results
  - the relative weight of the arguments may change, e.g., compliance with a process standard might be replaced by proven in use
- Therefore plan for multiple reports
  - Obtain agreement on the argument structure first
  - Use identification of evidence as management tool

Final Thoughts

Assurance case must

- Integrate design analyses focused on hazards and FMEA
- Be reviewable

Assurance case evaluation criteria are currently subjective

- Need more data on which subtle defects are worth analysis efforts
- Need more understanding of what makes reliability arguments sound

Assurance case patterns hold promise of capturing valid arguments and guiding reliability improvement efforts

Conclusions

Within conventional assurance reports the ‘chain of argument’ can often get lost

- But the argument is more important than the document!

Assurance cases have been found to be a useful basis for mapping out and evolving the structure of the arguments

- Provides a roadmap for a document or set of documents
- Provides a basis for discussion among engineers and between developers and assessors
- Creating outline arguments at the beginning of a project helps show progress towards a complete solution

Contact Information

Charles B. Weinstock

System of Systems Software Assurance

+1 412-268-7719

weinstock@sei.cmu.edu

Web: http://www.sei.cmu.edu/dependability/research/assurance/

U.S. mail:

Software Engineering Institute

Customer Relations

4500 Fifth Avenue

Pittsburgh, PA 15213-2612

USA

Customer Relations

Email:
customer-relations@sei.cmu.edu

Telephone: +1 412-268-5800

- NO WARRANTY
- THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.
- Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.
- This Presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.
- This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

Software Engineering Institute | Carnegie Mellon